

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-322328
 (43)Date of publication of application : 04.12.1998

(51)Int.Cl. H04L 9/32
 H04L 9/08
 H04L 12/28

(21)Application number : 09-130177
 (22)Date of filing : 20.05.1997

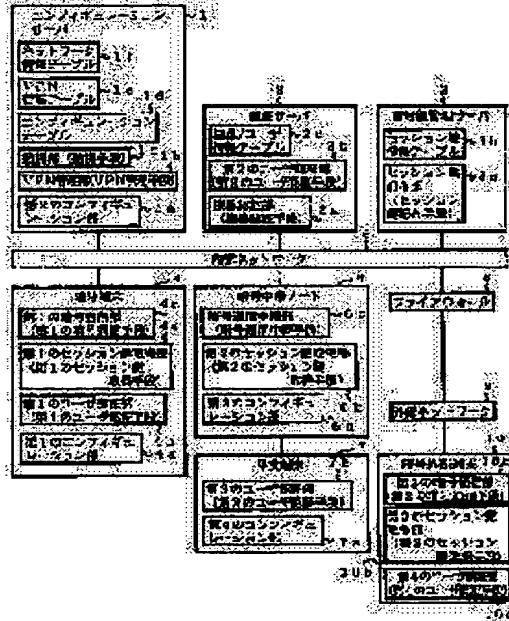
(71)Applicant : MITSUBISHI ELECTRIC CORP
 (72)Inventor : NAKAMURA HIROSHI
 SENO SHOICHIRO
 BABA YOSHIMASA
 OKAZAKI NAOYOSHI
 HIRAMATSU KOICHI
 FUJII TERUKO
 ATSUI YUJI

(54) ENCRYPTION COMMUNICATION SYSTEM AND ENCRYPTION COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain the encryption communication system and the encryption communication method with high security by making encryption virtual private network(VPN) communication after devices of each terminal and a relay node and the user using the devices are authenticated.

SOLUTION: An encryption terminal 4 receives configuration information from a configuration server 1 after receiving device authentication of an authentication server 2 and sets a network interface. When the user of the encryption terminal makes a request of encryption VPN communication, the configuration server 1 requests distribution of a session key to an encryption key management server 3 after being user-authenticated by the authentication server 2. The encryption terminal 4 uses the distributed session key to make the encryption VPN communication.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

[REPORT] [SEARCHER] [INFORMATION] [DETAIL] [INDEX]

1 / 1

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-322328

(43)公開日 平成10年(1998)12月4日

(51)Int.Cl.⁶
H 0 4 L 9/32
9/08
12/28

識別記号

F I
H 0 4 L 9/00
11/00

6 7 5 D
6 0 1 E
6 0 1 B
6 7 3 B
3 1 0 Z

審査請求 未請求 請求項の数13 O.L (全23頁)

(21)出願番号 特願平9-130177

(22)出願日 平成9年(1997)5月20日

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 中村 浩

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)発明者 妹尾 尚一郎

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)発明者 馬場 義昌

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(74)代理人 弁理士 田澤 博昭 (外1名)

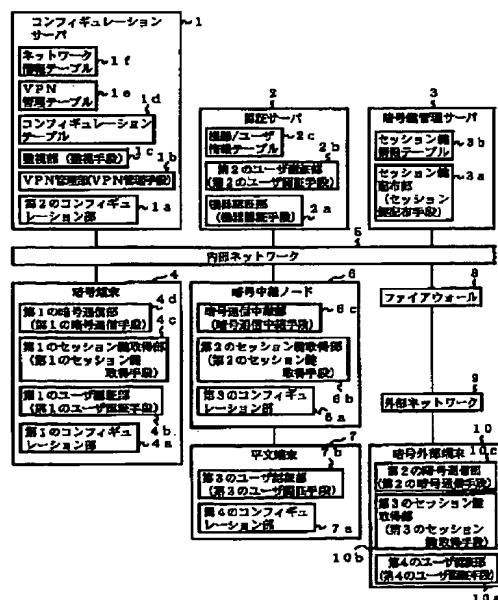
最終頁に続く

(54)【発明の名称】 暗号通信システム及び暗号通信方法

(57)【要約】

【課題】 暗号通信を行う機器が内部ネットワークへアクセスする場合、認証された特定の機器で、かつ認証された特定のユーザに制限することができないという課題があった。

【解決手段】 暗号端末4は認証サーバ2の機器認証を受けてから、コンフィギュレーションサーバ1よりコンフィギュレーション情報を受取り、ネットワークインターフェースを設定する。また暗号端末4のユーザが暗号VPN通信の要求を行うと、コンフィギュレーションサーバ1は、認証サーバ2のユーザ認証を受けてから、暗号鍵管理サーバ3にセッション鍵の配布を依頼する。暗号端末4は配布されたセッション鍵を用いて暗号VPN通信を行う。



1a: 第2のコンフィギュレーション部 (第2のコンフィギュレーション手段)
1b: 第1のコンフィギュレーション部 (第1のコンフィギュレーション手段)
1c: 第3のコンフィギュレーション部 (第3のコンフィギュレーション手段)
1d: 第4のコンフィギュレーション部 (第4のコンフィギュレーション手段)
2: 認証サーバ
2a: 第2のセッション鍵配布部 (第2のユーザ認証手段)
2b: 第2のユーザ認証部 (第2のユーザ認証手段)
3: 暗号鍵管理サーバ
3a: セッション鍵配布部 (セッション鍵配布手段)
3b: セッション鍵配布部 (セッション鍵配布手段)
4a: 暗号端末
4b: 第1のコンフィギュレーション部 (第1のユーザ認証手段)
4c: 第2のコンフィギュレーション部 (第2のユーザ認証手段)
4d: 第3のコンフィギュレーション部 (第3のユーザ認証手段)
5: 内田ネットワーク
6: ファイアウォール
7a: 第1のセッション鍵配布部 (第1のセッション鍵配布手段)
7b: 第2のセッション鍵配布部 (第2のセッション鍵配布手段)
7c: 第3のセッション鍵配布部 (第3のセッション鍵配布手段)
7d: 第4のセッション鍵配布部 (第4のセッション鍵配布手段)
8: 外部ネットワーク
9: 平文端末
10a: 第1のユーザ認証部 (第1のユーザ認証手段)
10b: 第2のユーザ認証部 (第2のユーザ認証手段)
11c: 第3のユーザ認証部 (第3のユーザ認証手段)

【特許請求の範囲】

【請求項1】 ネットワークに接続され、暗号通信を行う暗号端末と、
上記ネットワークに接続される上記暗号端末の機器認証とその機器を使用するユーザのユーザ認証を行う認証サーバと、
上記ネットワークに接続され、上記暗号端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配信するコンフィギュレーションサーバと、
上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備えた暗号通信システムにおいて、
上記暗号端末は、
上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第1のコンフィギュレーション手段と、
ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第1のユーザ認証手段と、
上記ユーザ認証の結果、上記暗号鍵管理サーバから上記暗号通信用のセッション鍵を取得する第1のセッション鍵取得手段と、
取得した上記セッション鍵を用いて暗号VPN通信を行う第1の暗号通信手段とを備え、
上記コンフィギュレーションサーバは、
上記第1のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号端末に上記コンフィギュレーション情報を配信する第2のコンフィギュレーション手段と、
上記第1のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段とを備え、
上記認証サーバは、
上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、
上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、
上記暗号鍵管理サーバは、
上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第1のセッション鍵取得手段に、上記セッ

ション鍵を配布するセッション鍵配布手段を備えたことを特徴とする暗号通信システム。

【請求項2】 ルータなどのネットワーク機器により構築されたネットワークと、
上記ネットワークに接続され、暗号通信を行う暗号端末と、
上記ネットワークに接続される上記暗号端末の機器認証とその機器を使用するユーザのユーザ認証を行う認証サーバと、
上記ネットワークに接続され、上記暗号端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配信すると共に、上記ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、
上記ネットワークに接続され、暗号通信用のセッション鍵を任意のタイミングで更新し配布する暗号鍵管理サーバとを備えた暗号通信システムにおいて、
上記暗号端末は、
上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第1のコンフィギュレーション手段と、
ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第1のユーザ認証手段と、
上記ユーザ認証の結果、上記暗号鍵管理サーバから上記暗号通信用のセッション鍵を取得すると共に、その後に任意のタイミングで更新されたセッション鍵を取得する第1のセッション鍵取得手段と、
取得した上記セッション鍵を用いて暗号VPN通信を行う第1の暗号通信手段とを備え、
上記コンフィギュレーションサーバは、
上記第1のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号端末に上記コンフィギュレーション情報を配信する第2のコンフィギュレーション手段と、
上記第1のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属VPN情報に基づき、上記ネットワーク機器に対し、上記暗号端末を使用するユーザが上記暗号VPN通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段とを備え、

上記認証サーバは、

上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、

上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、

上記暗号鍵管理サーバは、

上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第1のセッション鍵取得手段に、上記セッション鍵を配布すると共に、その後に任意のタイミングで更新されるセッション鍵を配布するセッション鍵配布手段を備えたことを特徴とする暗号通信システム。

【請求項3】 請求項2記載の暗号通信システムにおいて、上記コンフィギュレーションサーバは、上記暗号端末の暗号VPN通信の通信状況を把握する監視手段を備え、上記暗号端末が暗号VPN通信をしていない場合、上記監視手段は上記VPN管理手段に上記暗号端末のVPN離脱通知を行い、VPN離脱通知を受けた上記VPN管理手段は、上記暗号VPN通信を行うためのネットワーク設定を解除すると共に上記暗号鍵管理サーバにVPN離脱通知を行い、VPN離脱通知を受けた上記暗号鍵管理サーバは、上記暗号端末に対し、その後に任意のタイミングで更新されるセッション鍵の配布を中止することを特徴とする暗号通信システム。

【請求項4】 ネットワークに接続され、暗号通信を行う暗号端末と、

上記ネットワークに接続される上記暗号端末の機器認証とその機器を使用するユーザのユーザ認証を行う認証サーバと、

上記ネットワークに接続され、上記暗号端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送するコンフィギュレーションサーバと、

上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備えて通信を行う暗号通信方法において、

上記暗号端末が上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行うステップと、

上記コンフィギュレーションサーバが上記コンフィギュレーション情報の取得要求を受けて、上記認証サーバに上記機器認証の要求を行うステップと、

上記認証サーバが上記機器認証の要求を受けて機器の正当性を確認し、上記コンフィギュレーションサーバに機器認証の結果を通知するステップと、

上記コンフィギュレーションサーバが上記認証サーバからの機器認証を受け、上記暗号端末に上記コンフィギュレーション情報を配送するステップと、

上記暗号端末が配送された上記コンフィギュレーション

情報からネットワークインターフェースの設定を行うステップと、

上記暗号端末がユーザから与えられたユーザ認証情報を含んだVPN(Virtual Private Network)要求を上記コンフィギュレーションサーバに行うステップと、

上記コンフィギュレーションサーバが上記VPN要求を受けて、上記認証サーバに上記ユーザ認証の要求を行うステップと、

上記認証サーバが上記ユーザ認証の要求を受けてユーザの正当性を確認し、上記コンフィギュレーションサーバにユーザ認証の結果を通知するステップと、

上記コンフィギュレーションサーバが上記認証サーバからのユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するステップと、

上記暗号鍵管理サーバが上記セッション鍵の配布依頼を受け、上記暗号端末に上記セッション鍵を配布するステップと、

上記暗号端末が取得した上記セッション鍵を用いて上記暗号VPN通信を行うステップとを備えたことを特徴とする暗号通信方法。

【請求項5】 ネットワークに接続された暗号中継ノードの中継により通信を行う暗号機能を持たない平文端末と、

上記ネットワークに接続される上記暗号中継ノード及び上記平文端末の機器認証並びにその平文端末を使用するユーザのユーザ認証を行う認証サーバと、

上記ネットワークに接続され、上記暗号中継ノードと上記平文端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送するコンフィギュレーションサーバと、

上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備えた暗号通信システムにおいて、

上記暗号中継ノードは、

上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第3のコンフィギュレーション手段と、

上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得する第2のセッション鍵取得手段と、

取得した上記セッション鍵を用いて、上記平文端末との通信を中継し暗号通信を行う暗号通信中継手段とを備え、

上記平文端末は、

上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバによ

り上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第4のコンフィギュレーション手段と、

ユーザから与えられたユーザ認証情報を含んだV P N (Virtual Private Network)

要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第3のユーザ認証手段とを備え、

上記コンフィギュレーションサーバは、

上記第3及び第4のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号中継ノードと上記平文端末に上記コンフィギュレーション情報を配達する第2のコンフィギュレーション手段と、

上記第3のユーザ認証手段からのV P N要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するV P N管理手段とを備え、

上記認証サーバは、

上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、

上記V P N管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、

上記暗号鍵管理サーバは、

上記V P N管理手段からの上記セッション鍵の配布依頼を受け、上記第2のセッション鍵取得手段に上記セッション鍵を配布するセッション鍵配布手段を備えたことを特徴とする暗号通信システム。

【請求項6】 ルータなどのネットワーク機器により構築されたネットワークと、

上記ネットワークに接続された暗号中継ノードの中継により通信を行う暗号機能を持たない平文端末と、

上記ネットワークに接続される上記暗号中継ノード及び上記平文端末の機器認証並びにその平文端末を使用するユーザのユーザ認証を行う認証サーバと、

上記ネットワークに接続され、上記暗号中継ノードと上記平文端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配達すると共に、上記ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属V P N (Virtual Private Network)情報を管理するコンフィギュレーションサーバと、

上記ネットワークに接続され、暗号通信用のセッション鍵を任意のタイミングで更新し配布する暗号鍵管理サーバとを備えた暗号通信システムにおいて、

上記暗号中継ノードは、

上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第3のコンフィギュレーション手段と、

上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得すると共に、その後に任意のタイミングで更新されたセッション鍵を取得する第2のセッション鍵取得手段と、

取得した上記セッション鍵を用いて、上記平文端末との通信を中継し暗号通信を行う暗号通信中継手段とを備え、

上記平文端末は、

上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第4のコンフィギュレーション手段と、

ユーザから与えられたユーザ認証情報を含んだV P N (Virtual Private Network)

要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第3のユーザ認証手段とを備え、

上記コンフィギュレーションサーバは、

上記第3及び第4のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号中継ノードと上記平文端末に上記コンフィギュレーション情報を配達する第2のコンフィギュレーション手段と、

上記第3のユーザ認証手段からのV P N要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属V P N情報に基づき、上記ネットワーク機器に対し、上記平文端末を使用するユーザが暗号V P N通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するV P N管理手段とを備え、

上記認証サーバは、

上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、

上記V P N管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、

上記暗号鍵管理サーバは、

上記V P N管理手段からの上記セッション鍵の配布依頼を受け、上記第2のセッション鍵取得手段に、上記セッション鍵を配布すると共に、その後に任意のタイミング

で更新されたセッション鍵を配布するセッション鍵配布手段を備えたことを特徴とする暗号通信システム。

【請求項7】 請求項6記載の暗号通信システムにおいて、上記コンフィギュレーションサーバは、上記平文端末の暗号V PN通信の通信状況を把握する監視手段を備え、上記平文端末が暗号V PN通信をしていない場合、上記監視手段は上記V PN管理手段に上記平文端末のV PN離脱通知を行い、V PN離脱通知を受けた上記V PN管理手段は、上記暗号V PN通信を行うためのネットワーク設定を解除すると共に上記暗号鍵管理サーバにV PN離脱通知を行い、V PN離脱通知を受けた上記暗号鍵管理サーバは、上記暗号中継ノードに対し、その後に任意のタイミングで更新されるセッション鍵の配布を中止すると共に、すでに配布されているセッション鍵の削除通知を行うことを特徴とする暗号通信システム。

【請求項8】 ネットワークに接続された暗号中継ノードの中継により通信を行う暗号機能を持たない平文端末と、

上記ネットワークに接続される上記暗号中継ノード及び上記平文端末の機器認証並びにその平文端末を使用するユーザのユーザ認証を行う認証サーバと、

上記ネットワークに接続され、上記暗号中継ノードと上記平文端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配信するコンフィギュレーションサーバと、

上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備えて通信を行う暗号通信方法において、

上記暗号中継ノードが上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行うステップと、

上記コンフィギュレーションサーバが上記コンフィギュレーション情報の取得要求を受けて、上記認証サーバに上記機器認証の要求を行うステップと、

上記認証サーバが上記機器認証の要求を受けて機器の正当性を確認し、上記コンフィギュレーションサーバに機器認証の結果を通知するステップと、

上記コンフィギュレーションサーバが上記認証サーバからの機器認証を受け、上記暗号中継ノードに上記コンフィギュレーション情報を配信するステップと、

上記暗号中継ノードが配信された上記コンフィギュレーション情報からネットワークインターフェースの設定を行うステップと、

上記平文端末が上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行うステップと、

上記コンフィギュレーションサーバが上記平文端末からのコンフィギュレーション情報の取得要求を受けて、上記認証サーバに上記平文端末の機器認証の要求を行うステップと、

上記認証サーバが上記平文端末の機器認証の要求を受けて機器の正当性を確認し、上記コンフィギュレーションサーバに機器認証の結果を通知するステップと、
上記コンフィギュレーションサーバが上記認証サーバからの機器認証を受け、上記平文端末に上記コンフィギュレーション情報を配信するステップと、
上記平文端末が配信された上記コンフィギュレーション情報からネットワークインターフェースの設定を行うステップと、
上記平文端末がユーザから与えられたユーザ認証情報を含んだV PN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行うステップと、
上記コンフィギュレーションサーバが上記V PN要求を受けて、上記認証サーバに上記ユーザ認証の要求を行うステップと、
上記認証サーバが上記ユーザ認証の要求を受けてユーザの正当性を確認し、上記コンフィギュレーションサーバにユーザ認証の結果を通知するステップと、
上記コンフィギュレーションサーバが上記認証サーバからのユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するステップと、
上記暗号鍵管理サーバが上記セッション鍵の配布依頼を受け、上記暗号中継ノードに上記セッション鍵を配布するステップと、
上記暗号中継ノードが取得した上記セッション鍵を用いて、上記平文端末との通信を中継し上記暗号V PN通信を行うステップとを備えたことを特徴とする暗号通信方法。

【請求項9】 ルータなどのネットワーク機器により構築されたファイアウォールを介し内部ネットワークに接続された外部ネットワークと、

上記外部ネットワークに接続され、暗号通信を行う暗号外部端末と、

上記内部ネットワークに接続される上記暗号外部端末を使用するユーザのユーザ認証を行う認証サーバと、

上記内部ネットワークに接続され、上記内部ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属V PN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、上記内部ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備えた暗号通信システムにおいて、

上記暗号外部端末は、

ユーザから与えられたユーザ認証情報を含んだV PN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第4のユーザ認証手段と、

上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号

通信用のセッション鍵を取得する第3のセッション鍵取得手段と、

取得した前記セッション鍵を用いて暗号VPN通信を行う第2の暗号通信手段とを備え、

上記コンフィギュレーションサーバは、

上記第4のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属VPN情報に基づき、上記ファイアウォールを構築するネットワーク機器に対し、上記暗号外部端末を使用するユーザが上記暗号VPN通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段を備え、

上記認証サーバは、

上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段を備え、

上記暗号鍵管理サーバは、

上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第3のセッション鍵取得手段に、上記セッション鍵を配布するセッション鍵配布手段を備えたことを特徴とする暗号通信システム。

【請求項11】 ルータなどのネットワーク機器により構築された内部ネットワークと、

ルータなどのネットワーク機器により構築されたファイアウォールを介し上記内部ネットワークに接続された外部ネットワークと、

上記外部ネットワークに接続され、暗号通信を行う暗号外部端末と、

上記内部ネットワークに接続される上記暗号外部端末を使用するユーザのユーザ認証を行う認証サーバと、

上記内部ネットワークに接続され、上記内部ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、

上記内部ネットワークに接続され、暗号通信用のセッション鍵を任意のタイミングで更新し配布する暗号鍵管理サーバとを備えた暗号通信システムにおいて、

上記暗号外部端末は、

ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第4のユーザ認証手段と、

上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得すると共に、その後に任意のタイミングで更新されるセッション鍵を取得する第3のセッション鍵取得手段と、

取得した前記セッション鍵を用いて暗号VPN通信を行

う第2の暗号通信手段とを備え、

上記コンフィギュレーションサーバは、

上記第4のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属VPN情報に基づき、上記ネットワーク機器に対し、上記暗号外部端末を使用するユーザが上記暗号VPN通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段を備え、

上記認証サーバは、

上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段を備え、

上記暗号鍵管理サーバは、

上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第3のセッション鍵取得手段に、上記セッション鍵を配布すると共に、その後に任意のタイミングで更新されるセッション鍵を配布するセッション鍵配布手段を備えたことを特徴とする暗号通信システム。

【請求項12】 請求項10記載の暗号通信システムにおいて、上記コンフィギュレーションサーバは、上記暗号外部端末の暗号VPN通信の通信状況を把握する監視手段を備え、上記暗号外部端末が暗号VPN通信をしていない場合、上記監視手段は上記VPN管理手段に上記暗号外部端末のVPN離脱通知を行い、VPN離脱通知を受けた上記VPN管理手段は、上記暗号VPN通信を行うためのネットワーク設定を解除すると共に上記暗号鍵管理サーバにVPN離脱通知を行い、VPN離脱通知を受けた上記暗号鍵管理サーバは、上記暗号外部端末に対し、その後に任意のタイミングで更新するセッション鍵の配布を中止することを特徴とする暗号通信システム。

【請求項13】 請求項9または請求項10記載の暗号通信システムにおいて、上記コンフィギュレーションサーバは、上記暗号VPN通信に参加しているユーザ、使用機器、各暗号VPN通信の優先度及び上記ファイアウォールで使用する各暗号VPN通信の必要帯域を含んだVPN情報を格納したVPN管理テーブルを備え、上記VPN管理手段は、各暗号VPN通信の参加状況に応じ上記VPN管理テーブルのVPN情報を更新すると共に、上記各暗号VPNの優先度に応じて上記ファイアウォールのトラヒック制御を行うことを特徴とする暗号通信システム。

【請求項14】 ルータなどのネットワーク機器により構築されたファイアウォールを介し内部ネットワークに接続された外部ネットワークと、

上記外部ネットワークに接続され、暗号通信を行う暗号外部端末と、

上記内部ネットワークに接続され、上記内部ネットワークに介入する上記暗号外部端末を使用するユーザのユー

ザ認証を行う認証サーバと、

上記内部ネットワークに接続され、上記内部ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、

上記内部ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備えて通信を行う暗号通信方法において、

上記暗号外部端末がユーザから与えられたユーザ認証情報を持ったVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行うステップと、

上記コンフィギュレーションサーバが上記VPN要求を受けて、上記認証サーバに上記ユーザ認証の要求を行うステップと、

上記認証サーバが上記ユーザ認証の要求を受けてユーザの正当性を確認し、上記コンフィギュレーションサーバにユーザ認証の結果を通知するステップと、

上記コンフィギュレーションサーバが上記認証サーバからのユーザ認証を受け、上記所属VPN情報に基づき、上記ネットワーク機器に対し、上記暗号外部端末を使用するユーザが上記VPN要求による暗号VPN通信を行うためのネットワークの設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するステップと、上記暗号鍵管理サーバが上記セッション鍵の配布依頼を受け、上記暗号外部端末に上記セッション鍵を配布するステップと、

上記暗号外部端末が取得した上記セッション鍵を用いて上記暗号VPN通信を行うステップとを備えたことを特徴とする暗号通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号通信によりVPN (Virtual Private Network) を構築し、安全に相互接続を行う通信システムに係わり、特にセキュリティを確保するために、機器とユーザの認証後にセッション鍵の配布を行い、ネットワーク環境設定をVPN所属ユーザの有無に応じ動的に行う暗号通信システム及び暗号通信方法に関するものである。

【0002】

【従来の技術】図7はインターネット上の標準プロトコルを定めるIETF (Internet Engineering Task Force) のドキュメントに記載されている従来の暗号通信システムを示す構成図である。図7において、4は暗号通信機能を有する暗号端末、1はコンフィギュレーションサーバで、暗号端末4等のノードへネットワークインターフェースの設定を行うためのコンフィギュレーション情報の配布を行う。

3は上記各ノードへセッション鍵の配布を行う暗号鍵管理サーバ、5は内部ネットワークであり、6は暗号中継ノードで、暗号ゲートウェイなど暗号機能を有すると共に、他のノード例えは暗号通信機能を持たない平文端末7を収容し中継する。さらに8は外部ネットワーク9からの不要な侵入を防ぐファイアウォールであり、10はIP (Internet Protocol) アドレスが接続毎に変化しノードの識別を固定的にIPアドレスで識別できない暗号機能を有した暗号外部端末である。

【0003】次に動作について説明する。従来の暗号通信システムでは、暗号端末4は、ネットワークへのアクセス機器として設定されているものであれば、立ち上げ時に、RFC (Request For Comments) で規定されているようなDHCP (Dynamic Host Configuration Protocol-RFC1531) プロトコルや、BOOTP (Bootstrap Protocol-RFC1947) プロトコルなどによって、IP (Internet Protocol) ネットワークである内部ネットワーク5を介して、コンフィギュレーションサーバ1からネットワークインターフェースなどのコンフィギュレーション情報を受け取ることができる。

【0004】次に暗号端末4を使用するユーザは暗号鍵管理サーバ3から認証を受け、セッション鍵を取得し暗号VPNに参加する。

【0005】また、暗号VPNを構築するためのネットワーク環境は、ネットワーク管理者が、内部ネットワーク5を構築するルータ(図示せず)やファイアウォール8を構築するルータやゲートウェイ(図示せず)などのネットワーク機器に対して、個別に設定を行っており、外部ネットワーク9と接続する部分のファイアウォール8を介して、暗号外部端末10などの特定サーバの特定アプリケーションに対してのアクセスが可能になる。

【0006】

【発明が解決しようとする課題】従来の暗号通信システムは以上のように構成されているので、暗号端末4が立ち上げ時に、コンフィギュレーションサーバ1からコンフィギュレーション情報を得るが、その暗号端末4がネットワークアクセス機器として設定されていても、正規に許可された特定の機器かを認証する手段がなくセキュリティ強度が低い。またセキュリティ上、内部ネットワーク5へのアクセスを正規機器を使用した正規ユーザのみに制限したい場合に、暗号端末4を使用するユーザがその正規の暗号端末の使用を許可されているか否かの判断ができないという課題があった。

【0007】また、暗号機能を持たない平文端末7が、暗号ゲートウェイなど暗号機能を有した暗号中継ノード6に収容される場合、正規の平文端末か否かの判断ができない。さらにその平文端末7を使用するユーザがその正規の平文端末の使用を許可されているか否かの判断が

できないという課題があった。

【0008】さらに、外部ネットワーク9に接続され、外部ネットワーク9からIPアドレスを取得するため、接続の度にIPアドレスが変化するような暗号機能を有する暗号外部端末10が、内部ネットワーク5にアクセスする場合、その暗号外部端末10を使用するユーザが正規に許可されているか否かの判断ができないという課題があった。さらに、セキュリティ強度を低下させないためには、暗号鍵管理サーバ3からセッション鍵を配布後、必要時のみ、暗号外部端末10からのパケットがファイアウォール8を通過できるようにしなければならない。しかし従来の暗号通信システムでは、ファイアウォール8の設定を動的に更新することができないという課題があった。

【0009】さらに、暗号VPNに参加している暗号端末4、平文端末7、暗号外部端末10などのユーザが、暗号VPNに参加する必要が無くなった場合、ユーザのアクセスを禁止することができず、ネットワークでのセキュリティを確保できないという課題があった。

【0010】さらに、ファイアウォール8のトラヒック制御を暗号VPN単位で動的に行うために必要な制御情報の一元管理しておらず、ユーザの暗号VPNへの参加と離脱を動的に制御情報に反映できず、通信の優先度に応じた通信品質を確保できないという課題があった。

【0011】この発明は上記のような課題を解決するためになされたもので、各端末や中継ノードの機器認証とその機器を使用するユーザ認証を行ってから、暗号VPNによる通信を可能とすることにより、セキュリティ強度の高い暗号通信システム及び暗号通信方法を得ることを目的とする。

【0012】また、この発明は、暗号VPNに参加していた各端末のユーザが、暗号VPNに参加する必要が無くなった場合、ユーザのアクセスを禁止することにより、ユーザ認証を動的に更新し、ネットワークでのセキュリティを向上させた暗号通信システムを得ることを目的とする。

【0013】さらに、この発明は、ファイアウォール8のトラヒック制御を暗号VPN単位で動的に行い、暗号VPN通信の優先度に応じた通信品質を確保できる暗号通信システムを得ることを目的とする。

【0014】

【課題を解決するための手段】請求項1記載の発明に係る暗号通信システムは、ネットワークに接続され、暗号通信を行う暗号端末と、上記ネットワークに接続される上記暗号端末の機器認証とその機器を使用するユーザのユーザ認証を行う認証サーバと、上記ネットワークに接続され、上記暗号端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送するコンフィギュレーションサーバと、上記ネットワークに接続され、暗号通信用のセッション鍵を配布す

る暗号鍵管理サーバとを備え、上記暗号端末が、上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第1のコンフィギュレーション手段と、ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い上記認証サーバから上記ユーザ認証を受ける第1のユーザ認証手段と、上記ユーザ認証の結果、上記暗号鍵管理サーバから上記暗号通信用のセッション鍵を取得する第1のセッション鍵取得手段と、取得した上記セッション鍵を用いて暗号VPN通信を行う第1の暗号通信手段とを備え、上記コンフィギュレーションサーバが、上記第1のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号端末に上記コンフィギュレーション情報を配信する第2のコンフィギュレーション手段と、上記第1のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段とを備え、上記認証サーバが、上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、上記暗号鍵管理サーバが、上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第1のセッション鍵取得手段に、上記セッション鍵を配布するセッション鍵配布手段を備えたものである。

【0015】請求項2記載の発明に係る暗号通信システムは、ルータなどのネットワーク機器により構築されたネットワークと、上記ネットワークに接続され、暗号通信を行う暗号端末と、上記ネットワークに接続される上記暗号端末の機器認証とその機器を使用するユーザのユーザ認証を行う認証サーバと、上記ネットワークに接続され、上記暗号端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送すると共に、上記ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、上記ネットワークに接続され、暗号通信用のセッション鍵を任意のタイミングで更新し配布する暗号鍵管理サーバとを備え、上記暗号端末が、上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、

上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第1のコンフィギュレーション手段と、ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第1のユーザ認証手段と、上記ユーザ認証の結果、上記暗号鍵管理サーバから上記暗号通信用のセッション鍵を取得すると共に、その後に任意のタイミングで更新されるセッション鍵を取得する第1のセッション鍵取得手段と、取得した上記セッション鍵を用いて上記VPN要求による暗号VPN通信を行う第1の暗号通信手段とを備え、上記コンフィギュレーションサーバが、上記第1のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号端末に上記コンフィギュレーション情報を配送する第2のコンフィギュレーション手段と、上記第1のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属VPN情報に基づき、上記ネットワーク機器に対し、上記暗号端末を使用するユーザが上記暗号VPN通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段とを備え、上記認証サーバが、上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、上記暗号鍵管理サーバが、上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第1のセッション鍵取得手段に、上記セッション鍵を配布すると共に、その後に任意のタイミングで更新されるセッション鍵を配布するセッション鍵配布手段を備えたものである。

【0016】請求項3記載の発明に係る暗号通信システムは、コンフィギュレーションサーバが、暗号端末の暗号VPN通信の通信状況を把握する監視手段を備え、上記暗号端末が暗号VPN通信をしていない場合、上記監視手段がVPN管理手段に上記暗号端末のVPN離脱通知を行い、VPN離脱通知を受けた上記VPN管理手段が、上記暗号VPN通信を行うためのネットワーク設定を解除すると共に上記暗号鍵管理サーバにVPN離脱通知を行い、VPN離脱通知を受けた上記暗号鍵管理サーバが、上記暗号端末に対し、その後に任意のタイミングで更新されるセッション鍵の配布を中止するものである。

【0017】請求項4記載の発明に係る暗号通信方法は、ネットワークに接続され、暗号通信を行う暗号端末と、上記ネットワークに接続される上記暗号端末の機器

認証とその機器を使用するユーザのユーザ認証を行う認証サーバと、上記ネットワークに接続され、上記暗号端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送するコンフィギュレーションサーバと、上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備え、上記暗号端末が上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行うステップと、上記コンフィギュレーションサーバが上記コンフィギュレーション情報の取得要求を受けて、上記認証サーバに上記機器認証の要求を行うステップと、上記認証サーバが上記機器認証の要求を受けて機器の正当性を確認し、上記コンフィギュレーションサーバに機器認証の結果を通知するステップと、上記コンフィギュレーションサーバが上記認証サーバからの機器認証を受け、上記暗号端末に上記コンフィギュレーション情報を配送するステップと、上記暗号端末が配送された上記コンフィギュレーション情報からネットワークインターフェースの設定を行うステップと、上記暗号端末がユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行うステップと、上記コンフィギュレーションサーバが上記VPN要求を受けて、上記認証サーバに上記ユーザ認証の要求を行うステップと、上記認証サーバが上記ユーザ認証の要求を受けてユーザの正当性を確認し、上記コンフィギュレーションサーバにユーザ認証の結果を通知するステップと、上記コンフィギュレーションサーバが上記認証サーバからのユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するステップと、上記暗号鍵管理サーバが上記セッション鍵の配布依頼を受け、上記暗号端末に上記セッション鍵を配布するステップと、上記暗号端末が取得した上記セッション鍵を用いて上記暗号VPN通信を行うステップとを備えたものである。

【0018】請求項5記載の発明に係る暗号通信システムは、ネットワークに接続された暗号中継ノードの中継により通信を行う暗号機能を持たない平文端末と、上記ネットワークに接続される上記暗号中継ノード及び上記平文端末の機器認証並びにその平文端末を使用するユーザのユーザ認証を行う認証サーバと、上記ネットワークに接続され、上記暗号中継ノードと上記平文端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送するコンフィギュレーションサーバと、上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備え、上記暗号中継ノードが、上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフ

イギュレーション情報を取得し、上記ネットワークインターフェースを設定する第3のコンフィギュレーション手段と、上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得する第2のセッション鍵取得手段と、取得した上記セッション鍵を用いて、上記平文端末との通信を中継し暗号通信を行う暗号通信中継手段とを備え、上記平文端末が、上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第4のコンフィギュレーション手段と、ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第3のユーザ認証手段とを備え、上記コンフィギュレーションサーバが、上記第3及び第4のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号中継ノードと上記平文端末に上記コンフィギュレーション情報を配信する第2のコンフィギュレーション手段と、上記第3のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段とを備え、上記認証サーバが、上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、上記暗号鍵管理サーバが、上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第2のセッション鍵取得手段に上記セッション鍵を配布するセッション鍵配布手段を備えたものである。

【0019】請求項6記載の発明に係る暗号通信システムは、ルータなどのネットワーク機器により構築されたネットワークと、上記ネットワークに接続された暗号中継ノードの中継により通信を行う暗号機能を持たない平文端末と、上記ネットワークに接続される上記暗号中継ノード及び上記平文端末の機器認証並びにその平文端末を使用するユーザのユーザ認証を行う認証サーバと、上記ネットワークに接続され、上記暗号中継ノードと上記平文端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配信すると共に、上記ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、上記ネットワークに接続され、暗号通信用のセッション鍵を任意のタイミ

ングで更新し配布する暗号鍵管理サーバとを備え、上記暗号中継ノードが、上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第3のコンフィギュレーション手段と、上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得すると共に、その後に任意のタイミングで更新されるセッション鍵を取得する第2のセッション鍵取得手段と、取得した上記セッション鍵を用いて、上記平文端末との通信を中継し暗号通信を行う暗号通信中継手段とを備え、上記平文端末が、上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行い、上記認証サーバにより上記機器認証がされた場合、上記コンフィギュレーションサーバから上記コンフィギュレーション情報を取得し、上記ネットワークインターフェースを設定する第4のコンフィギュレーション手段と、ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第3のユーザ認証手段とを備え、上記コンフィギュレーションサーバが、上記第3及び第4のコンフィギュレーション手段からの上記コンフィギュレーション情報の取得要求により、上記認証サーバに上記機器認証の要求を行って機器認証を受け、上記暗号中継ノードと上記平文端末に上記コンフィギュレーション情報を配信する第2のコンフィギュレーション手段と、上記第3のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属VPN情報に基づき、上記ネットワーク機器に対し、上記平文端末を使用するユーザが上記VPN要求による暗号VPN通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段とを備え、上記認証サーバが、上記第2のコンフィギュレーション手段からの上記機器認証の要求を受けて機器の正当性を確認する機器認証手段と、上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段とを備え、上記暗号鍵管理サーバが、上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第2のセッション鍵取得手段に、上記セッション鍵を配布すると共に、その後に任意のタイミングで更新されるセッション鍵を配布するセッション鍵配布手段を備えたものである。

【0020】請求項7記載の発明に係る暗号通信システムは、コンフィギュレーションサーバが、平文端末の暗号VPN通信の通信状況を把握する監視手段を備え、上記平文端末が暗号VPN通信をしていない場合、上記監

視手段がV P N管理手段に上記平文端末のV P N離脱通知を行い、V P N離脱通知を受けた上記V P N管理手段が、上記暗号V P N通信を行うためのネットワーク設定を解除すると共に上記暗号鍵管理サーバにV P N離脱通知を行い、V P N離脱通知を受けた上記暗号鍵管理サーバが、上記暗号中継ノードに対し、その後に任意のタイミングで更新されるセッション鍵の配布を中止すると共に、すでに配布されているセッション鍵の削除通知を行うものである。

【0021】請求項8記載の発明に係る暗号通信方法は、ネットワークに接続された暗号中継ノードの中継により通信を行う暗号機能を持たない平文端末と、上記ネットワークに接続される上記暗号中継ノード及び上記平文端末の機器認証並びにその平文端末を使用するユーザのユーザ認証を行う認証サーバと、上記ネットワークに接続され、上記暗号中継ノードと上記平文端末のネットワークインターフェースを設定するために必要なコンフィギュレーション情報を配送するコンフィギュレーションサーバと、上記ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備え、上記暗号中継ノードが上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行うステップと、上記コンフィギュレーション情報の取得要求を受けて、上記認証サーバに上記機器認証の要求を行うステップと、上記認証サーバが上記機器認証の要求を受けて機器の正当性を確認し、上記コンフィギュレーションサーバに機器認証の結果を通知するステップと、上記コンフィギュレーションサーバが上記認証サーバからの機器認証を受け、上記暗号中継ノードに上記コンフィギュレーション情報を配送するステップと、上記暗号中継ノードが配送された上記コンフィギュレーション情報からネットワークインターフェースの設定を行うステップと、上記平文端末が上記コンフィギュレーションサーバに上記コンフィギュレーション情報の取得要求を行うステップと、上記コンフィギュレーションサーバが上記平文端末からのコンフィギュレーション情報の取得要求を受けて、上記認証サーバに上記平文端末の機器認証の要求を行うステップと、上記認証サーバが上記平文端末の機器認証の要求を受けて機器の正当性を確認し、上記コンフィギュレーションサーバに機器認証の結果を通知するステップと、上記コンフィギュレーションサーバが上記認証サーバからの機器認証を受け、上記平文端末に上記コンフィギュレーション情報を配送するステップと、上記平文端末が配送された上記コンフィギュレーション情報からネットワークインターフェースの設定を行うステップと、上記平文端末がユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行うステップと、上記コンフィギュレーションサーバ

が上記V P N要求を受けて、上記認証サーバに上記ユーザ認証の要求を行うステップと、上記認証サーバが上記ユーザ認証の要求を受けてユーザの正当性を確認し、上記コンフィギュレーションサーバにユーザ認証の結果を通知するステップと、上記コンフィギュレーションサーバが上記認証サーバからのユーザ認証を受け、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するステップと、上記暗号鍵管理サーバが上記セッション鍵の配布依頼を受け、上記暗号中継ノードに上記セッション鍵を配布するステップと、上記暗号中継ノードが取得した上記セッション鍵を用いて、上記平文端末との通信を中継し上記暗号V P N通信を行うステップとを備えたものである。

【0022】請求項9記載の発明に係る暗号通信システムは、ルータなどのネットワーク機器により構築されたファイアウォールを介し内部ネットワークに接続された外部ネットワークと、上記外部ネットワークに接続され、暗号通信を行う暗号外部端末と、上記内部ネットワークに接続される上記暗号外部端末を使用するユーザのユーザ認証を行う認証サーバと、上記内部ネットワークに接続され、上記内部ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属V P N (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、上記内部ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備え、上記暗号外部端末が、ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第4のユーザ認証手段と、上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得する第3のセッション鍵取得手段と、取得した前記セッション鍵を用いて上記V P N要求による暗号V P N通信を行なう第2の暗号通信手段とを備え、上記コンフィギュレーションサーバが、上記第4のユーザ認証手段からのV P N要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属V P N情報に基づき、上記ネットワーク機器に対し、上記暗号外部端末を使用するユーザが上記暗号V P N通信を行うためのファイアウォールを構築するネットワーク機器のネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するV P N管理手段を備え、上記認証サーバが、上記V P N管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段を備え、上記暗号鍵管理サーバが、上記V P N管理手段からの上記セッション鍵の配布依頼を受け、上記第3のセッション鍵取得手段に、上記セッション鍵を配布するセッション鍵配布手段を備えたものである。

【0023】請求項10記載の発明に係る暗号通信シス

システムは、ルータなどのネットワーク機器により構築された内部ネットワークと、ルータなどのネットワーク機器により構築されたファイアウォールを介し上記内部ネットワークに接続された外部ネットワークと、上記外部ネットワークに接続され、暗号通信を行う暗号外部端末と、上記内部ネットワークに接続される上記暗号外部端末を使用するユーザのユーザ認証を行う認証サーバと、上記内部ネットワークに接続され、上記内部ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、上記内部ネットワークに接続され、暗号通信用のセッション鍵を任意のタイミングで更新し配布する暗号鍵管理サーバとを備え、上記暗号外部端末が、ユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行い、上記認証サーバから上記ユーザ認証を受ける第4のユーザ認証手段と、上記ユーザ認証の結果、上記暗号鍵管理サーバから暗号通信用のセッション鍵を取得すると共に、その後に任意のタイミングで更新されたセッション鍵を取得する第3のセッション鍵取得手段と、取得した前記セッション鍵を用いて上記VPN要求による暗号VPN通信を行う第2の暗号通信手段とを備え、上記コンフィギュレーションサーバが、上記第4のユーザ認証手段からのVPN要求により、上記認証サーバに上記ユーザ認証の要求を行ってユーザ認証を受け、上記所属VPN情報に基づき、上記ネットワーク機器に対し、上記暗号外部端末を使用するユーザが上記暗号VPN通信を行うためのネットワーク設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するVPN管理手段を備え、上記認証サーバが、上記VPN管理手段からの上記ユーザ認証の要求を受けてユーザの正当性を確認する第2のユーザ認証手段と備え、上記暗号鍵管理サーバが、上記VPN管理手段からの上記セッション鍵の配布依頼を受け、上記第3のセッション鍵取得手段に、上記セッション鍵を配布すると共に、その後に任意のタイミングで更新されるセッション鍵を配布するセッション鍵配布手段を備えたものである。

【0024】請求項1記載の発明に係る暗号通信システムは、コンフィギュレーションサーバが、暗号外部端末の暗号VPN通信の通信状況を把握する監視手段を備え、上記暗号外部端末が暗号VPN通信をしていない場合、上記監視手段がVPN管理手段に上記暗号外部端末のVPN離脱通知を行い、VPN離脱通知を受けた上記VPN管理手段が、上記暗号VPN通信を行うためのネットワーク設定を解除すると共に上記暗号鍵管理サーバにVPN離脱通知を行い、VPN離脱通知を受けた上記暗号鍵管理サーバが、上記暗号外部端末に対し、その後に任意のタイミングで更新するセッション鍵の配布を中

止するものである。

【0025】請求項12記載の発明に係る暗号通信システムは、コンフィギュレーションサーバが、暗号VPN通信に参加しているユーザ、使用機器、各暗号VPN通信の優先度及びファイアウォールで使用する各暗号VPN通信の必要帯域を含んだVPN情報を格納したVPN管理テーブルを備え、上記VPN管理手段が、各暗号VPN通信の参加状況に応じ上記VPN管理テーブルのVPN情報を更新すると共に、上記各暗号VPNの優先度に応じて上記ファイアウォールのトラヒック制御を行うものである。

【0026】請求項13記載の発明に係る暗号通信方法は、ルータなどのネットワーク機器により構築されたファイアウォールを介し内部ネットワークに接続された外部ネットワークと、上記外部ネットワークに接続され、暗号通信を行う暗号外部端末と、上記内部ネットワークに接続される上記暗号外部端末を使用するユーザのユーザ認証を行う認証サーバと、上記内部ネットワークに接続され、上記内部ネットワークに収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN (Virtual Private Network) 情報を管理するコンフィギュレーションサーバと、上記内部ネットワークに接続され、暗号通信用のセッション鍵を配布する暗号鍵管理サーバとを備え、上記暗号外部端末がユーザから与えられたユーザ認証情報を含んだVPN (Virtual Private Network) 要求を上記コンフィギュレーションサーバに行うステップと、上記コンフィギュレーションサーバが上記VPN要求を受けて、上記認証サーバに上記ユーザ認証の要求を行うステップと、上記認証サーバが上記ユーザ認証の要求を受けてユーザの正当性を確認し、上記コンフィギュレーションサーバにユーザ認証の結果を通知するステップと、上記コンフィギュレーションサーバが上記認証サーバからのユーザ認証を受け、記所属VPN情報に基づき、上記ネットワーク機器に対し、上記暗号外部端末を使用するユーザが上記VPN要求による暗号VPN通信を行うためのネットワークの設定を行い、上記暗号鍵管理サーバに上記セッション鍵の配布を依頼するステップと、上記暗号鍵管理サーバが上記セッション鍵の配布依頼を受け、上記暗号外部端末に上記セッション鍵を配布するステップと、上記暗号外部端末が取得した上記セッション鍵を用いて上記暗号VPN通信を行うステップとを備えたものである。

【0027】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。図1はこの発明の暗号通信システムを示す構成図である。図1において、4は暗号通信機能を有する暗号端末、1はコンフィギュレーションサーバで、暗号端末4などの端末へネットワークインターフェースの設定を行うためのコンフィギュレーション情報の配布を行

うと共に、内部ネットワーク5に収容された機器情報、ユーザ情報を含む暗号通信を行うための所属VPN(Virtual Private Network)情報を管理する。また、2は機器認証とユーザ認証を行う認証サーバ、3はセッション鍵の配布を実施する暗号鍵管理サーバ、6は暗号中継ノードで、暗号ゲートウェイなど暗号機能を有すると共に他のノード、例えば暗号通信機能を持たない平文端末7を収容し中継する。さらに8は外部ネットワーク9からの不要な侵入を防ぐファイアウォールであり、10はIP(Internet Protocol)アドレスが接続毎に変化しノードの識別を固定的にIPアドレスで識別できない暗号機能を有した暗号外部端末である。

【0028】上記内部ネットワーク5には、コンフィギュレーションサーバ1、認証サーバ2、暗号鍵管理サーバ3、暗号端末4が接続されている。また、平文端末7が暗号中継ノード6を介し、さらには暗号外部端末10が外部ネットワーク9及びファイアウォール8を介して内部ネットワーク5にそれぞれ接続されている。

【0029】上記図1において、暗号端末4は以下のように構成されている。4aはコンフィギュレーションサーバ1からコンフィギュレーション情報を取得し、ネットワークインターフェースの設定を行う第1のコンフィギュレーション部(第1のコンフィギュレーション手段)、4bはユーザから与えられたユーザ認証情報を含むVPN参加要求を出力する第1のユーザ認証部(第1のユーザ認証手段)、4cは暗号鍵管理サーバ3からセッション鍵を取得する第1のセッション鍵取得部(第1のセッション鍵取得手段)、4dは取得したセッション鍵を使用して、同一暗号VPNに所属する他のノードと暗号通信を行う第1の暗号通信部(第1の暗号通信手段)である。

【0030】また上記図1において、コンフィギュレーションサーバ1は以下のように構成されている。1aは暗号端末4、暗号中継ノード6、平文端末7へコンフィギュレーション情報を配信する第2のコンフィギュレーション部(第2のコンフィギュレーション手段)、1bは暗号端末4、平文端末7及び暗号外部端末10の機器情報と、使用する通信プロトコルなどの通信情報を含む所属VPN情報を含むセッション鍵配布依頼を鍵管理サーバ3に送信するVPN管理部(VPN管理手段)、1cは暗号VPNの通信状況を把握する監視部(監視手段)、1dはコンフィギューション情報を所持したコンフィギュレーションテーブル、1eはVPN管理テーブルで、暗号端末4、平文端末7及び暗号外部端末10の機器情報、ユーザ情報及び使用する通信プロトコルなどの通信情報を含む所属VPN情報を所持している。また1fはネットワーク情報テーブルで、内部ネットワーク5に収容されているネットワーク機器に関する情報を所持している。

【0031】さらに上記図1において、認証サーバ2は以下のように構成されている。2aは機器の正当性を確認する機器認証部(機器認証手段)、2bはユーザの正当性を確認する第2のユーザ認証部(第2のユーザ認証手段)、2cは機器認証情報とユーザ認証情報を所持する機器/ユーザ情報テーブルである。

【0032】さらに上記図1において、暗号鍵管理サーバ3は以下のように構成されている。3aはセッション鍵を配布するセッション鍵配布部(セッション鍵配布手段)、3bはセッション鍵情報テーブルで、各暗号VPNで使用するセッション鍵と各端末やノードが暗号VPNで通信中か非通信中かの情報を所持している。

【0033】さらに上記図1において、暗号中継ノード6は、コンフィギュレーションサーバ1からコンフィギュレーション情報を取得し、ネットワークインターフェースの設定を行う第3のコンフィギュレーション部(第3のコンフィギュレーション手段)6a、セッション鍵を取得する第2のセッション鍵取得部(第2のセッション鍵取得手段)6b及び取得したセッション鍵を使用して暗号通信を行う暗号通信中継部(暗号通信中継手段)6cより構成されている。

【0034】さらに上記図1において、平文端末7は、コンフィギュレーションサーバ1からコンフィギュレーション情報を取得し、ネットワークインターフェイスの設定を行う第4のコンフィギュレーション部(第4のコンフィギュレーション手段)7a及びユーザ認証情報を含むVPN参加要求をコンフィギュレーションサーバ1に送信する第3のユーザ認証部(第3のユーザ認証手段)7bにより構成されている。

【0035】さらに上記図1において、暗号外部端末10は、ユーザから与えられたユーザ認証情報を含むVPN参加要求をコンフィギュレーションサーバ1に出力する第4のユーザ認証部(第4のユーザ認証手段)10a、セッション鍵を取得する第3のセッション鍵取得部(第3のセッション鍵取得手段)10b及び取得したセッション鍵を使用して暗号通信を行う第2の暗号通信部(第2の暗号通信手段)10cより構成されている。

【0036】実施の形態1、図2はこの発明の実施の形態1におけるシーケンス図を示している。以下の動作について図1の構成図及び図2のシーケンス図を用いて説明する。図2において、コンフィギュレーションサーバ1、認証サーバ2、暗号鍵管理サーバ3及び暗号端末4は図1のものと同等のものである。

【0037】暗号端末4の起動時に、暗号端末4の第1のコンフィギュレーション部4aはコンフィギュレーションサーバ1に対し、コンフィギュレーション情報取得要求S101を発行する。このコンフィギュレーション情報取得要求S101には、暗号端末4の機器が認識できるMAC(Media Access Control)アドレス及び機器認証情報が格納されている。コン

フィギュレーション情報取得要求S101を受信したコンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、認証サーバ2に対して暗号端末4のMACアドレス及び機器認証情報を含む機器認証要求S102を発行する。認証サーバ2の機器認証部2aは、機器/ユーザ情報テーブル2cのMACアドレス及び機器認証情報と、受け取った機器認証要求S102のMACアドレス及び機器認証情報を比較して機器の正当性を確認する。

【0038】上記機器認証において、暗号端末4とコンフィギュレーションサーバ1間や、コンフィギュレーションサーバ1と認証サーバ2間で、複数のパケットの送受信によりMACアドレスおよび機器認証情報をやり取りしても良い。また機器認証要求S102の内容は、セキュリティ強度を高くするために暗号化されていても良い。

【0039】認証サーバ2の該機器認証部2aは、機器認証後、コンフィギュレーションサーバ1に機器認証結果通知S103を送信する。コンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、受信した機器認証結果通知S103の認証結果が正規機器と判定されれば、コンフィギュレーションテーブル1dから、暗号端末4のコンフィギュレーション情報を読み出し、暗号端末4にコンフィギュレーション情報配信S104を行う。暗号端末4の第1のコンフィギュレーション部4aは、取得したコンフィギュレーション情報からネットワークインターフェースの設定を行う。以上により暗号端末4は内部ネットワーク5に対して、通常のネットワークアクセスが可能になる。

【0040】コンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、認証サーバ2から受信した機器認証結果通知S103の認証結果が不正機器と判定されれば、暗号端末4にコンフィギュレーション情報配信S104を行わないので、暗号端末4のネットワークアクセスは不可能となる。

【0041】暗号端末4が正規機器と認証され、ネットワークインターフェースの設定を行った後、暗号端末4の第1のユーザ認証部4bは、ユーザが暗号端末4を使用し暗号VPNに参加するに先立ち、ユーザから与えられたユーザ認証情報を含むVPN参加要求S105をコンフィギュレーションサーバ1に送信する。VPN参加要求S105を受信したコンフィギュレーションサーバ1のVPN管理部1bは、認証サーバ2へユーザ認証要求S106を発行する。認証サーバ2の第2のユーザ認証部2bは、機器/ユーザ情報テーブル2cのユーザ認証情報とコンフィギュレーションサーバ1から受信したユーザ認証要求S106のユーザ認証情報を比較してユーザの正当性を確認する。

【0042】認証サーバ2の第2のユーザ認証部2bは、ユーザ認証後、ユーザ認証結果通知S107をコン

フィギュレーションサーバ1に送信する。認証サーバ2の第2のユーザ認証部2bは、正規ユーザと認証した場合、ユーザ認証結果通知S107に、使用する通信プロトコルなどの通信情報を含む所属VPN情報とユーザ情報を含ませる。ユーザ認証結果通知S107を受けたコンフィギュレーションサーバ1のVPN管理部1bは、VPN管理テーブル1eに、暗号端末4の機器情報、ユーザ情報及び使用する通信プロトコルなどの通信情報を含む所属VPN情報を登録し、暗号端末4へVPN参加結果通知S108を行う。

【0043】またVPN管理部1bは、内部ネットワーク5を構築するルータ(図示せず)などやファイアウォール8を構築するルータ、ゲートウェイ(図示せず)などのネットワーク機器に対して、VPN管理テーブル1e及びネットワーク情報テーブル1fを参照して、暗号端末4を使用するユーザが暗号VPNで通信するためのネットワーク設定を実施する。なお内部ネットワーク5について、ネットワークのトラヒックやセキュリティに關し、ルータなどのネットワーク機器でパケットフィルタリングなどのネットワーク設定が不要である場合には、内部ネットワーク5を構築するネットワーク機器への設定を行わない。

【0044】さらにVPN管理部1bは、暗号端末4の機器情報と使用する通信プロトコルなどの通信情報を含む所属VPN情報を含むセッション鍵配布依頼S109を暗号鍵管理サーバ3に送信する。セッション鍵配布依頼S109を受信した暗号鍵管理サーバ3のセッション鍵配布部3aは、セッション鍵配布S110により、使用する通信プロトコルなどの通信情報を含む所属全VPN情報とセッション鍵情報テーブル3bから取り出した各暗号VPNで使用するセッション鍵とを暗号端末4に転送する。同時に、セッション鍵配布部3aは、セッション鍵情報テーブル3bを、暗号端末4が「暗号VPNで非通信中」から「暗号VPNで通信中」に更新する。

【0045】暗号鍵管理サーバ3は、その後、定時間毎など任意のタイミングで、セッション鍵を更新すると共に暗号VPNに所属している暗号端末4などのノードに更新したセッション鍵の配布を行う。

【0046】暗号端末4の第1のセッション鍵取得部4cは、セッション鍵配布S110を受信し、セッション鍵を取得して第1の暗号通信部4dに登録する。第1の暗号通信部4dでは登録されたセッション鍵を使用して、同一暗号VPNに所属する他のノードと暗号通信を行うことができる。また、第1の暗号通信部4dは取得した所属暗号VPN以外の通信に対して暗号化をしない平文で行う。

【0047】また、暗号端末4がアプリケーションサーバなどの場合には、ユーザから与えられるユーザ認証情報は第1のユーザ認証部4bにあらかじめ設定してお

き、第1のコンフィギュレーション部4aが、コンフィギュレーション情報の取得を完了後に、第1のユーザ認証部4bが自動的にVPN参加要求S105を送信することにより上記手順を行い、同一暗号VPNに所属するノードと暗号通信を行うことができる。

【0048】以上のように、この実施の形態1によれば、機器の認証とこの機器を使用するユーザの認証を行い、正規機器はコンフィギュレーション情報を得ることができ、しかも正規機器を使用しつつ正規ユーザと認証後、セッション鍵の配布を行うので、ユーザは暗号VPNによりネットワークを介して安全に暗号通信ができる。

【0049】実施の形態2、図3はこの発明の実施の形態2におけるシーケンス図を示している。以下この動作について、図1の構成図及び図3のシーケンス図を用いて説明する。図3において、コンフィギュレーションサーバ1、認証サーバ2、暗号鍵管理サーバ3、暗号中継ノード6及び平文端末7は図2のものと同等のものである。

【0050】まず暗号中継ノード6の第3のコンフィギュレーション部6aは、上記実施の形態1における暗号端末4と同様に、起動時にコンフィギュレーションサーバ1に対し、コンフィギュレーション情報取得要求S201を発行する。このコンフィギュレーション情報取得要求S201には、暗号中継ノード6の機器が認識できるMACアドレス及び機器認証情報が格納されている。コンフィギュレーション情報取得要求S201を受信したコンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、認証サーバ2に対して暗号中継ノード6のMACアドレス及び機器認証情報を含む機器認証要求S202を発行する。認証サーバ2の機器認証部2aは、機器/ユーザ情報テーブル2cのMACアドレス及び機器認証情報と、受け取った機器認証要求S202のMACアドレス及び機器認証情報を比較して機器の正当性を確認する。

【0051】認証サーバ2の機器認証部2aは、機器認証後、コンフィギュレーションサーバ1に機器認証結果通知S203を送信する。コンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、受信した機器認証結果通知S203の認証結果が正規機器と判定されていれば、コンフィギュレーションテーブル1dから、暗号中継ノード6のコンフィギュレーション情報を読み出し、暗号中継ノード6にコンフィギュレーション情報配送S204を行う。暗号中継ノード6の第3のコンフィギュレーション部6aは、取得したコンフィギュレーション情報からネットワークインターフェースの設定を行う。以上により暗号中継ノード6は内部ネットワーク5に対して通常のネットワークアクセスが可能になる。この時点では暗号中継ノード6の暗号通信中継部6cは収容する平文端末7のコンフィギュレーションに

関する通信とユーザ認証に関する通信に中継を制限する。

【0052】次に暗号中継ノード6に収容された平文端末7の第4のコンフィギュレーション部7aは、起動時にコンフィギュレーションサーバ1に対し、コンフィギュレーション情報取得要求S205を発行する。このコンフィギュレーション情報取得要求S205には、平文端末7の機器が認識できるMACアドレス及び機器認証情報が格納されている。コンフィギュレーション情報取得要求S205を受信したコンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、上記実施の形態1と同様に、認証サーバ2に対して機器認証要求S206を発行する。認証サーバ2は同様に平文端末7の機器の正当性を確認する。

【0053】認証サーバ2は、機器認証後、コンフィギュレーションサーバ1に機器認証結果通知S207を送信する。コンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、受信した機器認証結果通知S207の認証結果が正規機器と判定されれば、上記実施の形態1と同様に、平文端末4にコンフィギュレーション情報配送S208を行う。平文端末7の第4のコンフィギュレーション部7aは、取得したコンフィギュレーション情報からネットワークインターフェースの設定を行う。以上により平文端末7は内部ネットワーク5に対して、通常のネットワークアクセスが可能となる。

【0054】コンフィギュレーションサーバ1の第2のコンフィギュレーション部1aは、認証サーバ2から受信した機器認証結果通知S207の認証結果が不正機器と判定されれば、平文端末4にコンフィギュレーション情報配送S208を行わないので、平文端末7のネットワークアクセスは不可能となる。

【0055】平文端末7が正規機器と認証され、ネットワークインターフェースの設定を行った後、平文端末7の第3のユーザ認証部7bは、ユーザが平文端末7を使用し暗号VPNに参加するに先立ち、ユーザから与えられたユーザ認証情報を含むVPN参加要求S209をコンフィギュレーションサーバ1に送信する。VPN参加要求S209を受信したコンフィギュレーションサーバ1のVPN管理部1bは、上記実施の形態1と同様に、認証サーバ2へユーザ認証要求S210を発行する。認証サーバ2は同様にユーザの正当性を確認する。

【0056】認証サーバ2は、ユーザ認証後、ユーザ認証結果通知S211をコンフィギュレーションサーバ1に送信する。認証サーバ2の第2のユーザ認証部2bは、正規ユーザと認証した場合、ユーザ認証結果通知S211に、使用する通信プロトコルなどの通信情報を含む所属VPN情報とユーザ情報を含ませる。ユーザ認証結果通知S211を受けたコンフィギュレーションサーバ1のVPN管理部1bは、VPN管理テーブル1e

に、平文端末7の機器情報、ユーザ情報及び使用する通信プロトコルなどの通信情報を含む所属VPN情報を登録し、平文端末7へVPN参加結果通知S212を行う。

【0057】またVPN管理部1bは、内部ネットワーク5を構築するルータなどやファイアウォール8を構築するルータ、ゲートウェイなどのネットワーク機器に対して、VPN管理テーブル1e及びネットワーク情報テーブル1fを参照して、平文端末7を使用するユーザが暗号VPNで通信するためのネットワーク設定を実施する。なお内部ネットワーク5について、ネットワークのトラヒックやセキュリティに関し、ルータなどのネットワーク機器でパケットフィルタリングなどのネットワーク設定が不要である場合には、内部ネットワーク5を構築するネットワーク機器への設定を行わない。

【0058】さらにVPN管理部1bは平文端末7が暗号中継ノード6に収容されていることをネットワーク情報テーブル1fから調査し、暗号中継ノード6の機器情報と、平文端末7のユーザの使用する通信プロトコルなどの通信情報を含む所属VPN情報を含むセッション鍵配布依頼S213を暗号鍵管理サーバ3に送信する。この時コンフィギュレーションサーバ1は、暗号鍵管理サーバ3に対し、セッション鍵を平文端末7ではなく、暗号中継ノード6へ配布するよう依頼する。

【0059】セッション鍵配布依頼S213を受信した暗号鍵管理サーバ3のセッション鍵配布部3aは、セッション鍵配布S214により、使用する通信プロトコルなどの通信情報を含む所属全VPN情報をセッション鍵情報テーブル3bから取り出した各暗号VPNで使用するセッション鍵とを暗号中継ノード6に転送する。同時に、セッション鍵配布部3aは、セッション鍵情報テーブル3bを、暗号中継ノード6が「暗号VPNで非通信中」から「暗号VPNで通信中」に更新する。

【0060】暗号鍵管理サーバ3は、その後定時間毎など任意のタイミングで、セッション鍵を更新すると共に暗号VPNに所属している暗号中継ノード6などのノードに更新したセッション鍵の配布を行う。

【0061】暗号中継ノード6の第2のセッション鍵取得部6bは、セッション鍵配布S214を受信し、セッション鍵を取得し、暗号通信中継部6cに登録する。暗号通信中継部6cではセッション鍵の登録を契機に、セッション鍵を使用して平文端末7が接続されたポートに対してコンフィギュレーションパケットとユーザ認証パケット以外のパケットの暗号化および復号化と中継処理を開始する。このようにして平文端末7は、同一暗号VPNに所属する他のノードと通信を行うことができる。また、暗号通信中継部6cは取得した所属暗号VPN以外の通信に対して暗号化をしない平文で行う。

【0062】また、平文端末7がアプリケーションサーバなどの場合には、ユーザから与えられるユーザ認証情

報は、第3のユーザ認証部7bにあらかじめ設定しており、第4のコンフィギュレーション部7aが、コンフィギュレーション情報の取得を完了後に、第3のユーザ認証部7bが自動的にVPN参加要求S209を送信することにより上記手順を行っても、同様に同一暗号VPNに所属する他のノードと暗号通信を行うことができる。

【0063】以上のように、この実施の形態2によれば、暗号ゲートウェイなど暗号機能を有する暗号中継ノードが、暗号機能を持たないノード（平文端末）を収容する場合、収容したノードと、そのノードを使用するユーザが正規と認証された後に、暗号VPN用のセッション鍵を配布するので、暗号機能を持たない既存のノードを使用するユーザが、暗号VPNによりネットワークを介して安全に通信ができる。

【0064】実施の形態3. 図4はこの発明の実施の形態3におけるシーケンス図を示している。以下この動作について、図1の構成図及び図4のシーケンス図を用いて説明する。図4において、コンフィギュレーションサーバ1、認証サーバ2、暗号鍵管理サーバ3、暗号外部端末10は図1のものと同等のものである。

【0065】暗号外部端末10は、内部ネットワーク5に適合したネットワークインターフェースなどの設定に必要なコンフィギュレーション情報が不要なため、コンフィギュレーションサーバ1からコンフィギュレーション情報を得ることなく、VPN参加要求S301からシーケンスを開始する。暗号外部端末10の第4のユーザ認証部10aは、ユーザが暗号外部端末10を使用し暗号VPNに参加するに先立ち、ユーザから与えられたユーザ認証情報を含むVPN参加要求S301を、コンフィギュレーションサーバ1に送信する。VPN参加要求S301を受信したコンフィギュレーションサーバ1のVPN管理部1bは、暗号外部端末10のIPアドレスを記憶し、暗号外部端末10が外部ネットワーク9に接続されており、使用機器とユーザとの組み合わせによる認証が必要ないことを含むユーザ認証要求S302を認証サーバ2へ発行する。

【0066】認証サーバ2の第2のユーザ認証部2bは、機器/ユーザ情報テーブル2cのユーザ認証情報とコンフィギュレーションサーバ1から受信したユーザ認証要求S302のユーザ認証情報を比較してユーザの正当性を確認し、ユーザ認証結果通知S303をコンフィギュレーションサーバ1に送信する。認証サーバ2のユーザ認証部2bは正規ユーザと認証した場合、ユーザ認証結果通知S303に使用する通信プロトコルなどの通信情報を含む所属VPN情報をユーザ情報と含ませる。ユーザ認証結果通知S303を受けたコンフィギュレーションサーバ1のVPN管理部1bは、VPN管理テーブル1eに、暗号外部端末10の機器情報、ユーザ情報及び使用する通信プロトコルなどの通信情報を含む所属VPN情報を登録する。そしてVPN管理部1b

は、暗号外部端末10へVPN参加結果通知S304を行う。

【0067】またVPN管理部1bは、内部ネットワーク5を構築するルータなどやファイアウォール8を構築するルータ、ゲートウェイなどのネットワーク機器に対して、VPN管理テーブル1e及びネットワーク情報テーブル1fを参照して、暗号外部端末を使用するユーザが暗号VPNで通信するためのネットワーク設定を実施する。なお内部ネットワーク5について、ネットワークのトラヒックやセキュリティに関し、ルータなどのネットワーク機器でパケットフィルタリングなどのネットワーク設定が不要である場合には、内部ネットワーク5を構築するネットワーク機器への設定を行わない。

【0068】さらにVPN管理部1bは、暗号外部端末10の機器情報と使用する通信プロトコルなどの通信情報を含む所属VPN情報を含むセッション鍵配布依頼S305を鍵管理サーバ3に送信する。セッション鍵配布依頼S305を受信した鍵管理サーバ3のセッション鍵配布部3aは、セッション鍵配布S306により、使用する通信プロトコルなどの通信情報を含む所属全VPN情報とセッション鍵情報テーブル3bから取り出した各暗号VPNで使用するセッション鍵とを暗号外部端末10に転送する。同時に、セッション鍵配布部3aは、セッション鍵情報テーブル3bを、暗号外部端末10が「暗号VPNで非通信中」から「暗号VPNで通信中」に更新する。このセッション鍵の配布にはコンフィギュレーションサーバ1のVPN管理部1bから通知されたIPアドレスを使用する。

【0069】暗号鍵管理サーバ3は、その後定時間毎など任意のタイミングで、セッション鍵を更新すると共に暗号VPNに所属している暗号外部端末10などのノードに更新したセッション鍵の配布を行う。

【0070】暗号外部端末10の第3のセッション鍵取得部10bは、セッション鍵配布S306を受信し、セッション鍵を取得し、第2の暗号通信部10cに登録する。第2の暗号通信部10cでは登録されたセッション鍵を使用して、同一暗号VPNに所属する他のノードと暗号通信を行うことができる。また、第2の暗号通信部10cは取得した所属暗号VPN以外の通信に対して暗号化をしない平文で行う。

【0071】以上のように、この実施の形態3によれば、外部ネットワークに位置し、外部ネットワークからIPアドレスを取得するため、接続の度にIPアドレスが変化するような暗号機能を有する暗号外部端末が、内部ネットワークにアクセスする時に、暗号外部端末のIPアドレスを記憶し、ユーザの認証を行い、ファイアウォールの設定を動的に更新し、セッション鍵の配布を行うので、暗号外部端末のユーザが暗号VPNにより外部ネットワークを介して安全に通信ができる。

【0072】実施の形態4、図5はこの発明の実施の形

態4におけるシーケンス図を示している。以下この動作について、図1の構成図及び図5のシーケンス図を用いて説明する。図5において、コンフィギュレーションサーバ1、暗号鍵管理サーバ3、暗号中継ノード6、平文端末7及び暗号外部端末10は図1のものと同等のものである。

【0073】コンフィギュレーションサーバ1の監視部1cは、暗号VPNの通信状況を把握するため、一定間隔で暗号外部端末10にVPN監視S401を送信する。暗号外部端末10の第4のユーザ認証部10aは、VPN監視S401を受信するとVPN監視S401に対するVPN監視応答S402を送信する。また暗号外部端末10のユーザ認証部10aは、コンフィギュレーションサーバ1からVPN監視S401を一定時間受信しない場合、コンフィギュレーションサーバ1にVPN継続要求S403を送信し、暗号VPNにより通信していることを通知する。

【0074】このように各ノードの暗号VPN所属意志の確認は、コンフィギュレーションサーバ1が、ポーリングにより一定間隔でユーザが暗号VPNに所属しているかを問い合わせるか、または一定間隔で暗号VPN所属中を示す通知を受けることにより行える。

【0075】コンフィギュレーションサーバ1の監視部1cは、暗号外部端末10から一定回数のVPN監視応答S402を受信しない場合で、かつVPN継続要求S403を受信しない場合、暗号外部端末10のユーザが暗号VPNに所属する必要がないと判断し、VPN管理部1bに暗号外部端末10のVPN離脱を通知し、暗号外部端末10を使用するユーザの削除を要求する。

【0076】またVPN管理部1bは、内部ネットワーク5を構築するルータなどやファイアウォール8を構築するルータ、ゲートウェイなどのネットワーク機器に対して、ネットワーク再設定を実施する。以降暗号外部端末10のVPN通信のパケットはファイアウォール8で廃棄される。

【0077】また同時にVPN管理部1bはVPN管理テーブル1eに格納しているVPN管理情報を更新し、暗号鍵管理サーバ3に機器情報と所属VPN情報を含むVPN離脱通知S404を送信し、暗号外部端末10を使用するユーザが暗号VPNに所属しないことを通知する。VPN離脱通知S404を受信した暗号鍵管理サーバ3のセッション鍵配布部3aは、セッション鍵情報テーブル3bを、暗号外部端末10が「暗号VPNで通信中」から「暗号VPNで非通信中」に更新する。暗号鍵管理サーバ3は、定時間毎など任意のタイミングで、セッション鍵を更新すると共に暗号VPNに所属する暗号外部端末10などのノードに更新したセッション鍵の配布を行ってきたが、暗号外部端末10が「暗号VPNで非通信中」となると、暗号外部端末10へ更新したセッション鍵の配布を行わない。セッション鍵の更新以降、

暗号外部端末10は暗号VPN通信が不可能となる。

【0078】図5には示していないが、暗号端末4がVPN離脱をする場合についても暗号外部端末10の場合と同様であり、暗号端末4のユーザはVPN離脱後セッション鍵が更新されると暗号VPN通信が不可能となる。

【0079】暗号中継ノード6に平文端末7が収容されている場合には、平文端末7の第3のユーザ認証部7bは、暗号外部端末10の第4のユーザ認証部10aと同様に、図5に示すように、VPN監視S401、VPN監視応答S402及びVPN継続要求S403の各送受信を行うことによって、暗号VPNにより通信していることを通知する。

【0080】コンフィギュレーションサーバ1の監視部1cは、平文端末7から一定回数のVPN監視応答S402を受信しない場合で、かつVPN継続要求S403を受信しない場合、平文端末7のユーザが暗号VPNに所属する必要がないと判断し、VPN管理部1bに平文端末7のVPN離脱を通知する。VPN管理部1bはVPN管理テーブル1e及びネットワーク情報テーブル1fを参照して、内部ネットワーク5を構築するルータなどやファイアウォール8を構築するルータ、ゲートウェイなどのネットワーク機器に対して、ネットワーク再設定を実施する。

【0081】また同時にVPN管理部1bは、平文端末7が暗号中継ノード6に収容されていることをネットワーク情報テーブル1fから調査し、VPN管理テーブル1eを更新し、暗号鍵管理サーバ3に平文端末7を収容する暗号中継ノード6の機器情報を含むVPN離脱通知S404を送信し、平文端末7を使用するユーザが暗号VPNに所属しないことを通知する。

【0082】VPN離脱通知S404を受信した暗号鍵管理サーバ3のセッション鍵配布部3aは、セッション鍵テーブル3bを、暗号中継ノード6が「暗号VPNで通信中」から「暗号VPNで非通信中」に更新する。暗号鍵管理サーバ3は、定時間毎など任意のタイミングで、セッション鍵を更新すると共に暗号VPNに所属する暗号中継ノード6などのノードに更新したセッション鍵の配布を行っていたが、暗号中継ノード6が「暗号VPNで非通信中」となれば、暗号中継ノード6に更新したセッション鍵の配布を行わない。

【0083】同時に暗号鍵管理サーバ3のセッション鍵配布部3aは、暗号中継ノード6に対して機器情報を含むVPN削除通知S405を送信する。すなわち暗号鍵管理サーバ3のセッション鍵配布部3aは、平文端末7が暗号VPNに所属しなくなった場合、平文端末7を収容する暗号中継ノード6に平文端末7を暗号VPNから削除することを通知する。これは平文端末7が暗号VPNで非通信となったことを暗号中継

ノード6に知らせて、その後の平文端末からの不要な中継を行うことを防ぐものである。

【0084】第2のセッション鍵取得部6bが暗号中継ノード6のVPN削除通知S405を受信したことを契機にして、それ以降、暗号中継ノード6の暗号通信中継部6cは、収容する平文端末7の通信のうち、コンフィギュレーションに関する通信とユーザ認証に関する通信に中継を限定する。

【0085】以上のように、この実施の形態4によれば、暗号VPNに参加しているユーザが使用するノードを監視して、暗号VPNに参加しているユーザが暗号VPNに参加する必要が無くなった時点で、ユーザのアクセスを禁止することにより、ネットワークでのセキュリティを確保できる。

【0086】実施の形態5、図6はこの発明の実施の形態5におけるコンフィギュレーションサーバ1のVPN管理テーブル1eが所持している情報内容を示す図である。以下図6を用いて説明する。

【0087】図6に示すように、VPN管理テーブル1eは、ユーザ毎の個別情報1e1と暗号VPN毎のファイアウォールにおける共通VPN制御情報1e2とを所持、すなわち暗号VPNに参加しているユーザと使用機器とVPN情報を所持している。図1におけるコンフィギュレーションサーバ1のVPN管理部1bは、図4におけるユーザ認証結果通知S303を受信すると、ユーザ認証結果通知S303の情報から、VPN管理テーブル1eのユーザ毎の個別情報1e1を更新するが、同時に個別情報1e1から、暗号VPN毎のファイアウォールにおける共通VPN制御情報1e2も更新する。共通VPN制御情報1e2には、暗号VPN毎に、暗号VPNの優先度、暗号VPNに参加している全ユーザがファイアウォール8で使用する必要帯域の合計値、ユーザ数等が格納されている。

【0088】共通VPN制御情報1e2の必要帯域の合計値と優先度から、コンフィギュレーションサーバ1のVPN管理部1bは、暗号VPN毎にファイアウォール8に対しトラヒック制御に使用する送信スケジュール情報を指定することができる。またファイアウォールと外部ネットワークとの接続帯域が、全暗号VPNの必要帯域合計の総計値より小さい場合には、VPN管理部1bは優先度の低い暗号VPNの必要帯域の合計を削減して、暗号VPN毎に、トラヒック制御に使用する送信スケジュール情報をファイアウォールに対し指定すれば、優先的に転送したい暗号VPNの通信品質を確保できる。送信スケジュール情報の算出については、使用的なファイアウォールに係わり、算出アルゴリズムは個別に所持しなければならずこの発明の範囲外であるが、暗号VPN毎に必要な情報を共通VPN制御情報1e2に格納しておけば対応可能である。

【0089】以上のように、この実施の形態5によれ

ば、ユーザ毎の個別情報と暗号V P N毎のファイアウォールにおける共通V P N制御情報を一元管理し、ファイアウォール8のトラヒック制御を暗号V P N単位で動的に行うことにより、暗号V P N通信の優先度に応じた通信品質を確保できる。

【0090】

【発明の効果】以上のように、請求項1記載の発明によれば、暗号端末の認証後にコンフィギュレーション情報を得てネットワークへのアクセスを可能とし、認証された暗号端末を使用するユーザの認証後に、セッション鍵の配布を行い、暗号V P Nによる通信を行うように構成したので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0091】請求項2記載の発明によれば、暗号端末の認証後にコンフィギュレーション情報を得てネットワークへのアクセスを可能とし、認証された暗号端末を使用するユーザの認証後に、ネットワークを構築しているネットワーク機器の設定を行ってセッション鍵の配布を行い、暗号V P Nによる通信を行うように構成したので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0092】請求項3記載の発明によれば、暗号V P Nに参加しているユーザが使用する暗号端末を監視して、暗号V P Nに参加しているユーザが暗号V P Nに参加する必要が無くなった時点で、その後のユーザのアクセスを禁止するようにしたので、正規に許可された以外のアクセスを禁止でき、ネットワークでのセキュリティを確保できる効果がある。

【0093】請求項4記載の発明によれば、暗号端末の認証後にコンフィギュレーション情報を得てネットワークへのアクセスを可能とし、認証された暗号端末を使用するユーザの認証後に、セッション鍵の配布を行い、暗号V P Nによる通信を行うようにしたので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0094】請求項5記載の発明によれば、暗号機能を有する暗号中継ノードの認証後にコンフィギュレーション情報を得て暗号中継ノードのネットワークへのアクセスを可能とし、暗号中継ノードに収容された暗号機能を持たない平文端末の認証後にコンフィギュレーション情報を得て平文端末のネットワークへのアクセスを可能とし、認証された平文端末を使用するユーザの認証後に、暗号中継ノードにセッション鍵の配布を行い、暗号V P Nによる通信を行うように構成したので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0095】請求項6記載の発明によれば、暗号機能を有する暗号中継ノードの認証後にコンフィギュレーション情報を得て暗号中継ノードのネットワークへのアクセスを可能とし、暗号中継ノードに収容された暗号機能を持たない平文端末の認証後にコンフィギュレーション情報を得て平文端末のネットワークへのアクセスを可能と

し、認証された平文端末を使用するユーザの認証後に、ネットワークを構築しているネットワーク機器の設定を行って暗号中継ノードにセッション鍵の配布を行い、暗号V P Nによる通信を行うように構成したので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0096】請求項7記載の発明によれば、暗号V P Nに参加しているユーザが使用する平文端末を監視して、暗号V P Nに参加しているユーザが暗号V P Nに参加する必要が無くなった時点で、その後のユーザのアクセスを禁止するようにしたので、正規に許可された以外のアクセスを禁止でき、ネットワークでのセキュリティを確保できる効果がある。

【0097】請求項8記載の発明によれば、暗号機能を有する暗号中継ノードの認証後にコンフィギュレーション情報を得て暗号中継ノードのネットワークへのアクセスを可能とし、暗号中継ノードに収容された暗号機能を持たない平文端末の認証後にコンフィギュレーション情報を得て平文端末のネットワークへのアクセスを可能とし、認証された平文端末を使用するユーザの認証後に、暗号中継ノードにセッション鍵の配布を行い、暗号V P Nによる通信を行うようにしたので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0098】請求項9の発明によれば、暗号外部端末を使用するユーザの認証後に、ファイアウォールを構築しているネットワーク機器の設定を行ってセッション鍵の配布を行い、暗号V P Nによる通信を行うように構成したので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0099】請求項10の発明によれば、暗号外部端末を使用するユーザの認証後に、内部ネットワークやファイアウォールを構築しているネットワーク機器の設定を行ってセッション鍵の配布を行い、暗号V P Nによる通信を行うように構成したので、ユーザはネットワークを介して安全に通信ができる効果がある。

【0100】請求項11記載の発明によれば、暗号V P Nに参加しているユーザが使用する暗号外部端末を監視して、暗号V P Nに参加しているユーザが暗号V P Nに参加する必要が無くなった時点で、その後のユーザのアクセスを禁止するので、正規に許可された以外のアクセスを禁止でき、ネットワークでのセキュリティを確保できる効果がある。

【0101】請求項12記載の発明によれば、ファイアウォールのトラヒック制御に必要な情報を一元管理し、ファイアウォールのトラヒック制御を暗号V P N単位で動的に行うように構成したので、暗号V P Nの優先度に応じた通信品質を確保できる効果がある。

【0102】請求項13の発明によれば、暗号外部端末を使用するユーザの認証後に、ファイアウォールを構築しているネットワーク機器の設定を行ってセッション鍵

の配布を行い、暗号VPNによる通信を行うようにしたので、ユーザはネットワークを介して安全に通信ができる効果がある。

【図面の簡単な説明】

【図1】 この発明の暗号通信システムを示す構成図である。

【図2】 この発明の実施の形態1を示すシーケンス図である。

【図3】 この発明の実施の形態2を示すシーケンス図である。

【図4】 この発明の実施の形態3を示すシーケンス図である。

【図5】 この発明の実施の形態4を示すシーケンス図である。

【図6】 この発明の実施の形態5によるコンフィギュレーションサーバのVPN管理テーブルを示す図である。

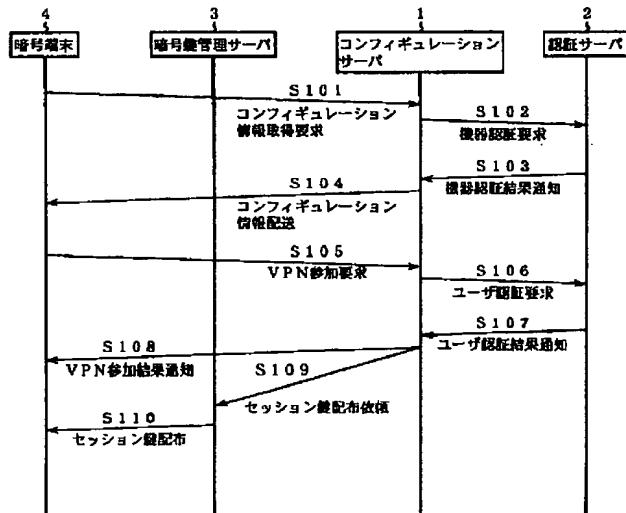
【図7】 従来の暗号通信システムを示す構成図である。

【符号の説明】

1 コンフィギュレーションサーバ、1 a 第2のコンフィギュレーション部（第2のコンフィギュレーション手段）、1 b VPN管理部（VPN管理手段）、1 c

監視部（監視手段）、1 e VPN管理テーブル、2 認証サーバ、2 a 機器認証部（機器認証手段）、2 b 第2のユーザ認証部（第2のユーザ認証手段）、3 暗号鍵管理サーバ、3 a セッション鍵配布部（セッション鍵配布手段）、4 暗号端末、4 a 第1のコンフィギュレーション部（第1のコンフィギュレーション手段）、4 b 第1のユーザ認証部（第1のユーザ認証手段）、4 c 第1のセッション鍵取得部（第1のセッション鍵取得手段）、4 d 第1の暗号通信部（第1の暗号通信手段）、5 内部ネットワーク、6 暗号中継ノード、6 a 第3のコンフィギュレーション部（第3のコンフィギュレーション手段）、6 b 第2のセッション鍵取得部（第2のセッション鍵取得手段）、6 c 暗号通信中継部（暗号通信中継手段）、7 平文端末、7 a 第4のコンフィギュレーション部（第4のコンフィギュレーション手段）、7 b 第3のユーザ認証部（第3のユーザ認証手段）、8 ファイアウォール、9 外部ネットワーク、10 暗号外部端末、10 a 第4のユーザ認証部（第4のユーザ認証手段）、10 b 第3のセッション鍵取得部（第3のセッション鍵取得手段）、10 c 第2の暗号通信部（第2の暗号通信手段）。

【図2】

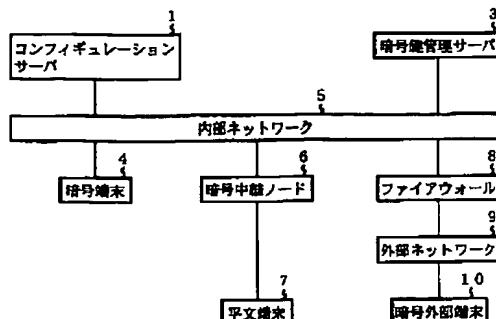


【図6】

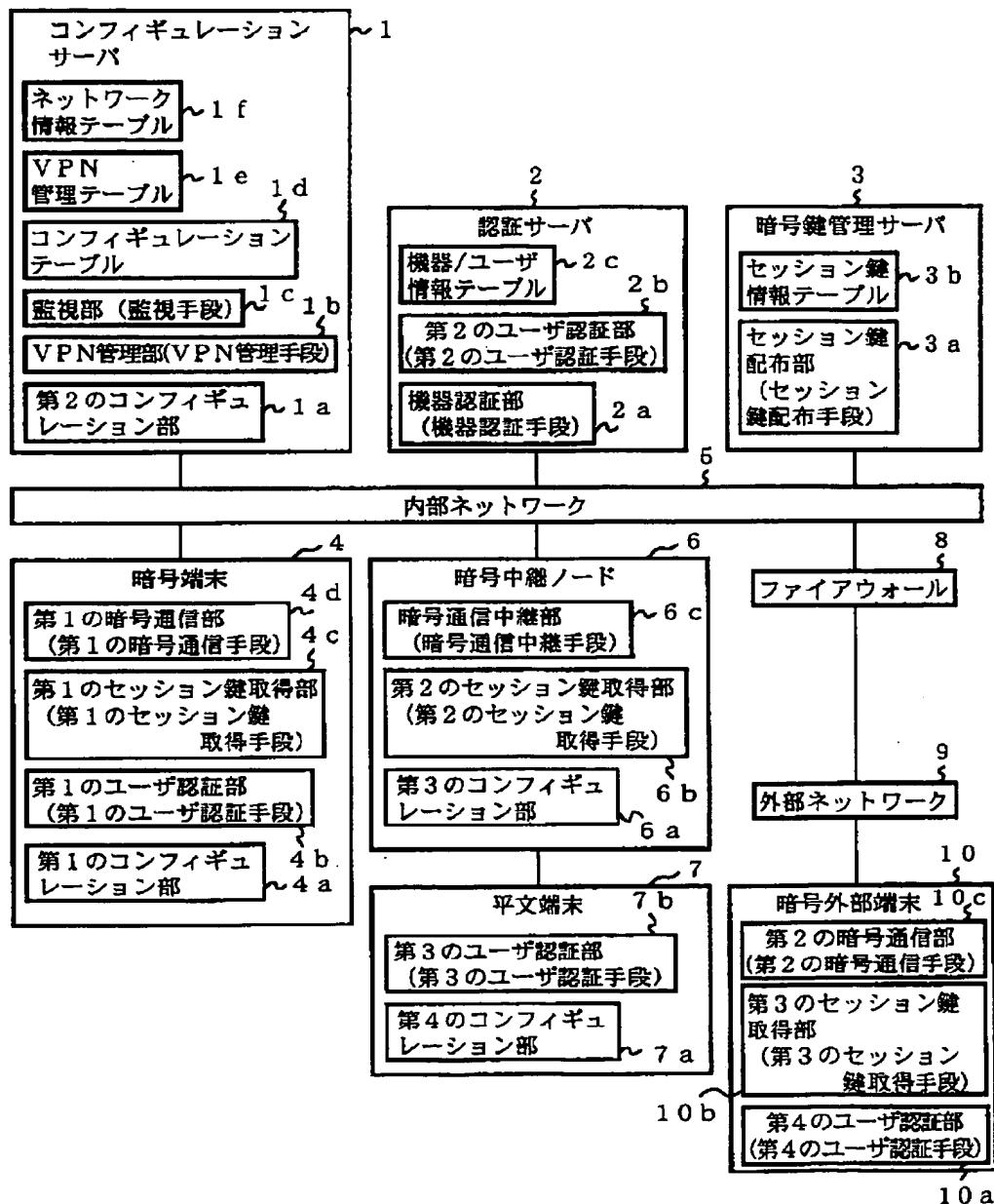
VPN管理テーブル			
個別情報			
ユーザ識別子	U1	----	Ux
VPN識別子	Vm	----	Vn
機密鍵識別子	Em	----	En
ネットワーク識別子	Nm	----	Nn

共通VPN割り当て情報			
VPN識別子	V1	----	Vx
VPN優先度	VPm	----	VPn
VPN許可帯域	MAXm	----	MAXn
プロトコル	PROTOCOLm	----	PROTOCOLn
ポート番号	PORTm	----	PORTn
フラグ	FLAGm	----	FLAGn
ファイアウォール帯域合計	RATEm	----	RATEn
ユーザ数	USERNOM	----	USERNON

【図7】



【図1】



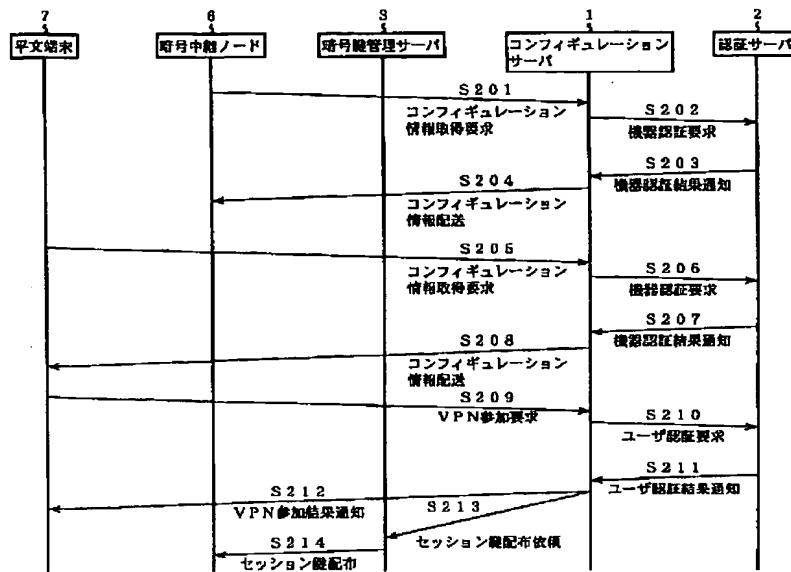
1 a : 第2のコンフィギュレーション部 (第2のコンフィギュレーション手段)

4 a : 第1のコンフィギュレーション部 (第1のコンフィギュレーション手段)

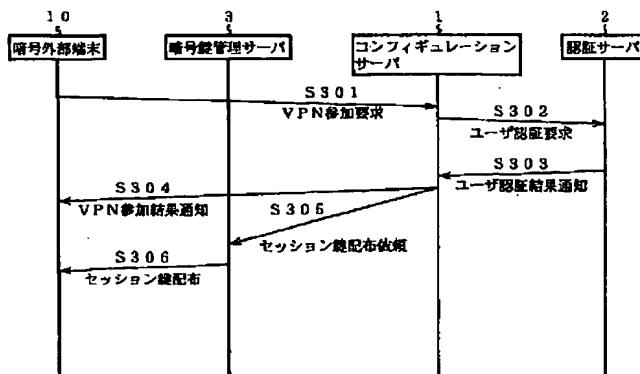
6 a : 第3のコンフィギュレーション部 (第3のコンフィギュレーション手段)

7 a : 第4のコンフィギュレーション部 (第4のコンフィギュレーション手段)

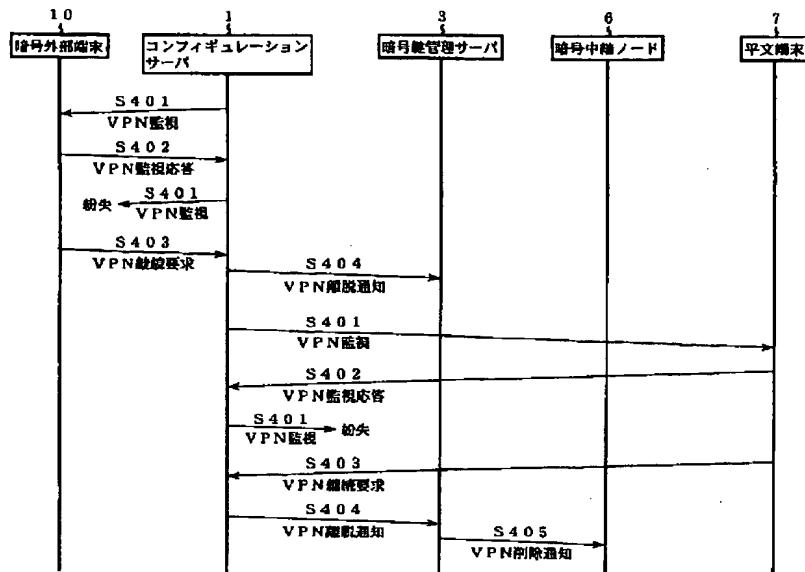
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者 岡崎 直宜
 東京都千代田区丸の内二丁目2番3号 三
 菱電機株式会社内

(72)発明者 平松 晃一
 東京都千代田区丸の内二丁目2番3号 三
 菱電機株式会社内

(72)発明者 藤井 照子
 東京都千代田区丸の内二丁目2番3号 三
 菱電機株式会社内

(72)発明者 厚井 裕司
 東京都千代田区丸の内二丁目2番3号 三
 菱電機株式会社内